CLAIMS

I claim:

1. A method of authenticating computing devices on a communications network comprising the steps of:

   receiving a first challenge from a computing device, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device;

   obtaining a first secret cryptographic key associated with said unique identifier;

   generating a second random number;

   decrypting said first random number with said first secret cryptographic key;

   encrypting said second random number with said first secret cryptographic key; and

   transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number.

2. The method of claim 1, wherein said unique identifier is a serial number of a physical token installed at said computing device.

3. The method of claim 2, wherein said step of obtaining a first secret cryptographic key comprises the step of

   retrieving a pre-stored record associated with said serial number, wherein said record comprises said first secret cryptographic key.

4. The method of claim 3, wherein said step of obtaining a first secret cryptographic key comprises the step of

   receiving a key database file comprising a number of records, wherein each record is associated with a unique physical token and comprises a unique secret cryptographic key and a unique serial number.

5. The method of claim 4, wherein said unique secret cryptographic key is created from a random number generated at initialization of said token.

6. The method of claim 1, further comprising the steps of:

   decrypting said first challenge with a network receive cryptographic key; and

   encrypting said second challenge with a network send cryptographic key.

7. The method of claim 3, wherein said step of decrypting said encrypted first random number results in a first value, and further comprising the step of

   disallowing said computing device to communicate with other computing devices on said network if said first value is a null value.

8. The method of claim 7, wherein

   allowing said computing device to communicate with other computing devices on said network if said first value is not a null value.

9. The method of claim 7, further comprising the step of

   decrypting said second challenge with a network receive cryptographic key.

10. The method of claim 8, further comprising the step of

    decrypting said encrypted second random number with a second secret cryptographic key.

11. The method of claim 10, wherein said second secret cryptographic key is stored within said physical token.

12. A method of deriving a new encryption key for a communication session comprising the steps of claim 1, and the step of

    transposing said first secret cryptographic key into said new encryption key, wherein said step of transposing comprises the steps of:

    calculating a modulus N of the first random number to obtain a result n;

    calculating a modulus N of the second random number to obtain a result m;

    equating the first bit of said new encryption key to the n-th bit of said secret cryptographic key; and

    equating the second bit of said new encryption key to the (n+m)th bit of said secret cryptographic key.

13. A communications system comprising:

    a number of computing devices, and

    at least one authentication device,

    wherein each client device or authentication device includes a unique tamper-resistant physical token comprising

    a random number generator,

a unique secret cryptographic key, and

and a unique serial number.

14. The system of claim 13, wherein each client device or authentication device further includes a wireless communications transceiver to communicate on a wireless network.
15. The system of claim 14, wherein said wireless network is Wi-Fi network.
16. The system of claim 15, wherein said authentication device is an access point.
17. The system of claim 13, wherein each tamper-resistant physical token is installed via a USB interface.
18. The system of claim 16, wherein said access point includes a database file comprising said serial numbers and secret cryptographic keys associated with said tokens.
19. A method of authenticating computing devices on a communications network comprising the steps of:

    receiving a first challenge from a computing device, wherein said first challenge comprises a first random number and a unique identifier associated with said computing device;

    obtaining a first secret cryptographic key associated with said unique identifier;

    generating a second random number;

    encrypting said first random number with said first secret cryptographic key; and

    transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number.
20. The method of claim 19, wherein said unique identifier is a serial number of a physical token installed at said computing device.
21. The method of claim 20, wherein said step of obtaining a first secret cryptographic key comprises the step of

    retrieving a pre-stored record associated with said serial number, wherein said record comprises said first secret cryptographic key.
22. The method of claim 21, wherein said step of obtaining a first secret cryptographic key comprises the step of

    receiving a key database file comprising a number of records, wherein each record is associated with a unique physical token and comprises a unique secret cryptographic key and a unique serial number.

23. The method of claim 22, wherein said unique secret cryptographic key is created from a random number generated at initialization of said token.

24. The method of claim 19, further comprising the steps of:

decrypting said first challenge with a network receive cryptographic key; and

encrypting said second challenge with a network send cryptographic key.

25. The method of claim 21, further comprising the steps of:

receiving a third challenge from said computing device, wherein said third challenge comprises said second random number encrypted with a second secret cryptographic key;

decrypting said encrypted second random number with said first secret cryptographic key; and

comparing said decrypted second random number to said second random number to determine if a match exists.

26. The method of claim 25, wherein

if a match exists between said decrypted second random number and said second random number,

allowing said computing device to communicate with other computing devices on said network,

otherwise if a match does not exist,

disallowing said computing device to communicate with other computing devices on said network.

27. The method of claim 25, further comprising the step of

decrypting said third challenge with a network receive cryptographic key.

28. The method of claim 25, wherein said second secret cryptographic key is stored within said physical token.